DESIGN METHODS AND PRACTICES FOR FAULT PREVENTION AND MANAGEMENT IN SPACECRAFT

Irem Y. Tumer, PhD
Lead, Complex Systems Design Group
Discovery and Systems Health Technical Area
Intelligent Systems Division
NASA Ames Research Center
Moffett Field, CA

ABSTRACT

Integrated Systems Health Management (ISHM) is intended to become a critical capability for all space, lunar and planetary exploration vehicles and systems at NASA. Monitoring and managing the health state of diverse components, subsystems, and systems is a difficult task that will become more challenging when implemented for long-term, evolving deployments. A key technical challenge will be to ensure that the ISHM technologies are reliable, effective, and low cost, resulting in turn in safe, reliable, and affordable missions. To ensure safety and reliability, ISHM functionality, decisions and knowledge have to be incorporated into the product lifecycle as early as possible, and ISHM must be considered as an essential element of models developed and used in various stages during system design. During early stage design, many decisions and tasks are still open, including sensor and measurement point selection, modeling and model-checking, diagnosis, signature and data fusion schemes, presenting the best opportunity to catch and prevent potential failures and anomalies in a cost-effective way. Using appropriate formal methods during early design, the design teams can systematically explore risks without committing to design decisions too early. However, the nature of ISHM knowledge and data is detailed, relying on high-fidelity, detailed models, whereas the earlier stages of the product lifecycle utilize low-fidelity, high-level models of systems and their functionality. We currently lack the tools and processes necessary for integrating ISHM into the vehicle system/subsystem design. As a result, most existing ISHM-like technologies are retrofits that were done after the system design was completed. It is very expensive, and sometimes futile, to retrofit a system health management capability into existing systems. Last-minute retrofits result in unreliable systems, ineffective solutions, and excessive costs (e.g., Space Shuttle TPS monitoring which was considered only after 110 flights and the Columbia disaster). High false alarm or false negative rates due to substandard implementations hurt the credibility of the ISHM discipline. This paper presents an overview of the current state of ISHM design and a review of formal design methods to make recommendations about possible approaches to enable the ISHM capabilities to be designed-in at the system-level, from the very beginning of the vehicle design process.

1 INTRODUCTION

The various vehicles and systems needed for NASA's exciting new mission to explore the moon and Mars need an intelligent and autonomous way to detect, diagnose, and recover from failures. Integrated Systems Health Management (ISHM) has been recognized as one of the critical technologies to achieve this goal. The ISHM capability needs to be safe, reliable, and affordable. To date, all existing ISHM efforts have been retrofits, implemented ad-hoc without the required insight from the system designers. It is expensive, and often futile, to retrofit system health management capability into an existing system as an after-thought. Experience in many domains has shown that high false alarm rates or false negative rates due to the lack of sensor data and/or inaccurate models to diagnose a problem hurt the credibility of the ISHM discipline. To meet the objectives of safety, reliability, and affordability, ISHM figures of merit, design criteria, and functional requirements must be incorporated into the overall system design as early as possible.

Specifically, to ensure robust day-to-day operation, ISHM systems *must* be integrated with their intended systems starting from the early design stages.

What is needed is to design ISHM functionality as an integral part of the vehicles and their systems' functionality, as early as possible, enabling an integrated ISHM design at the functional vehicle design stage. The need to consider ISHM as an essential function of the overall system from the very beginning has been recognized throughout the community and has been a topic of discussion in many briefings. Air Force Research Laboratories (AFRL), for example, is conducting a thorough "Design Study" to explore and evaluate the benefits of including ISHM in the early stages of design. Industry leaders such as Honeywell and Northrop Grumman have recognized this need and worked with NASA through various projects specifically on this aspect of ISHM. Early influence on system design by ISHM will guide the choice of whether to eliminate failure by design (through part selection and built-in redundancy), by prognosis leading to preventative maintenance, or by fault management (by ongoing diagnosis and recovery). In the shuttle AHMS program, for example, the Propulsion Synergy Team's final report recommends the engine health management systems be an integral piece of the engine design from the beginning and not an add-on. However, we currently lack formal methods and tools for integrating ISHM into the vehicle system/subsystem design.

In this light, this paper presents a survey of the state-of-the-practice and the state-of-the-art in design methods and system engineering practices, with the purpose of identifying methods and practices that have the potential to integrate ISHM design with the design of the systems they are intended to keep safe and reliable. We begin with a discussion of lifecycle considerations that must be taken into account when designing ISHM systems. We identify three major challenges that will hinder the efforts in achieving a robust ISHM design. We follow with a discussion of methods and tools developed in the design theory and methodology community, and discuss the potential of adopting these for ISHM design, followed with a discussion on the need to start failure and risk analysis activities in early design, and present various methods from the risk and reliability communities that need to be moved into the earlier stages of the design process. We then present a means to embed ISHM design, failure and risk analyses into the early stages of functional design. We then present some industry attempts to do a system-level design of ISHM systems, including design for testability and system analysis and optimization. followed by a collection of methodologies under development that draw from these ideas to address the need for system level design, analysis, and optimization of ISHM systems. The intent of the paper is to discuss ongoing efforts that can be used to achieve robust ISHM design, discuss their strong points and shortcomings, and present key recommendations for building robust and well integrated ISHM systems.

2 LIFECYCLE CONSIDERATIONS FOR ISHM DESIGN

For ambitious NASA programs such as Constellation, formal tools and methodologies need to be in place to allow program managers and lower level designers to formulate a clear understanding of the impact of the decisions in the downstream phases such as operations and maintenance on the systems design, and the impact of the decisions in the design phase on the operations and maintenance phases. These trades should be made during the early design phase with all the data and experts available instead of after the design and testing process is completed, and as such, provide significant savings in cost and reduction in risk. If NASA's Exploration mission is to be realized within available resources, it cannot afford to follow the example of previous major programs where operations and maintenance costs and risks became much larger than initially projected during Phase A initial design. In addition to supporting the design of reliable systems, with the ability to respond to failures during operations and hooks for system maintenance, the initial design must be examined in the context of the full system life cycle, with all stakeholders involved in the design, and the solution optimized in terms of well-defined Figures of Merit (FOMs). A depiction of the role of ISHM in the mission lifecycle is shown in Figure 1. Some examples where maintainability and supportability requirements were introduced in the early design phase with success, and lessons learned from past and current programs are as follows:

- For the Orbital Space Program (OSP) program, the contractors specified a service module that was not maintainable, and did not have a hatch to access certain components. A lesson learned was that

for maintainability, repair needs to be a factor in all phases of design. Experience from past programs showed that unplanned maintenance was a major driver in high operations costs.

- One of the most successful programs in terms of reducing life cycle costs is the Boeing-777 airliner. During a review of the 777 IVHM system with Honeywell and Boeing, it was learned that a large portion of this success was attributed to the fact that they successfully drove the operations requirements by having the chief mechanic elevated to the same approval level as the Chief Engineer. Both must sign off on a design before it can be incorporated.
- For the B-2 bomber program, a major finding was that component or subsystem supportability specialist, design engineers, and maintenance personnel should jointly establish requirements and perform analyses, ensuring early involvement of all users, and hand the results to the systems engineering team to compile a system level picture.
- On the F-35 Joint Strike Fighter Program, Northrop Grumman Integrated Systems applied its tradition of "designing-in" maintainability and supportability features for aircraft intended to operate effectively in harsh field environments. The concept of Autonomic Logistics [1] was used for planning life cycle cost efficiencies for the F-35. The approach is one of Operations Research applied to Logistics analysis and application of industry standard models such as CALM and LCOM. The Supportability Analysis team effectively applies a wide range of modeling tools to studies related to aircraft availability/sortie generation rates, maintenance manpower planning, Logistic Footprint and support costs, mission reliability, and more.

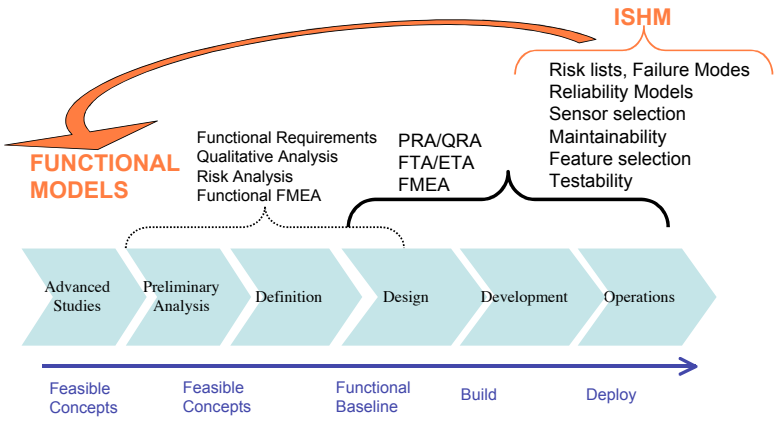

Figure 1: ISHM in the Mission Lifecycle.

3 DESIGN METHODS AND PRACTICES FOR ISHM DESIGN

Various methods and tools have been deployed at NASA and in industry to enhance design, which might aid in integrating ISHM design with system-level design. In addition, many design approaches have been published in the literature that enable the formalization of the design process. In the following, these methods and tools will be introduced and discussed in the context of ensuring the design of robust ISHM systems.

We first present key challenges facing the ISHM design community. We then summarize methods in the design research community that address these challenges. We follow with a discussion of reliability-based methods typically used at NASA and in industry as candidates for ISHM early design stage methodologies to assess risk and failures, focusing in particular on Probabilistic Risk Assessment (PRA), Fault Tree Analysis (FTA), and Failure Modes and Effects Analysis (FMEA). We then introduce an approach to

embed ISHM design into the earlier stages of system-wide functional design. We finally present methods for system analysis and optimization to enable the assessment of ISHM figures of merit on the overall system figures of merit. In this discussion, we present the Design for Testability (DFT) concept and its use in industry for sensor placement and ISHM design overall, present industry (namely, two prominent ISHM technology drivers, Honeywell and Northrop Grumman) and NASA efforts in optimizing ISHM design. We next introduce a multi-objective and multi-disciplinary optimization framework necessary to accurately evaluate the system figures of merit for the ISHM system and the overall vehicle system.

3.1 Key ISHM design Challenges

There are currently three major challenges facing ISHM design:

1. Embedding ISHM design into the earlier stages of functional design at the system level.
2. Moving failure, reliability, and risk analyses into the earlier stages of design.
3. Enabling analysis and optimization of the system-level and subsystem-level Figures of Merit.

The tools and methods presented in this section attempt to address these key challenges.

3.2 Tools and Methods from the Formal Design Methods Research Community

The Design Theory and Methodology research community has been producing a very large number of ideas to formalize and automate the design process. Most of these ideas are first published in the American Society of Mechanical Engineers' (ASME) International Design Engineering Technical Conferences, followed by various ASME journals including Journal of Mechanical Design and Journal of Computing and Information Science in Engineering. Some of the possible tools are risk visualization, multi-objective optimization, multi-level hierarchical risk minimization, human-guided design steering, and decision-based design [2]. Visualization can support designers by graphically presenting the space of possible designs and providing tools to examine the structure of the design space. An example is the DDP tool [3], a risk analysis tool developed at JPL, follows this route and adds interaction to bar charts and risk plots to analyze complex risk data. Optimization techniques such as multi-objective optimization can help solve the problem of multiple (and sometimes conflicting) objectives and constraints, and can be explored to provide tradeoffs between multiple design criteria. Despite the multiobjective nature of aerospace systems, there are very few papers that take a multiobjective design optimization approach to address them [4]. Multi-level hierarchical abstraction of NASA systems can help understand and define the objectives, variables, and constraints at both system and subsystem levels. An example is the Bi-Level Integrated System Synthesis (BLISS) that optimizes complex systems in a bi-level function [5]. Computational and design steering techniques can make use of automated and manual search that take advantage of the computer's ability to search rapidly and the human's ability to search using knowledge that is not easily formulated into a numeric objective measure. An example is intelligent interfaces to allow designers to select from a set of search algorithms, monitor running algorithms and re-order constraints in a configuration design application [6]. Finally, decision based design techniques can be used to help with objective and structured decision making processes using decision-theoretic interpretations of risk and uncertainty management in the context of design [7].

3.3 Reliability-Based Design Methods

NASA currently employs a number of reliability tools and methods, including FMEA/FMECA, FTA and PRA, and design engineers have used them successfully for designing reliable and safe systems. Traditionally, NASA engineers and managers use reliability methods during the design process to locate critical subsystems or components in a design. Failure and risk analysis methods range from traditional reliability-based tools to more recent probabilistic risk assessment (PRA) methods. Periodically a system is evaluated for failures as a whole, as it is during various design reviews. Analysis results identify how the likelihood of failure might be reduced through design changes [8-12].

Probabilistic risk analysis (PRA) methods provide a framework to guide design decision-making during the design process. This approach to risk assessment answers three questions: what can go wrong, how frequently will it happen and what are the consequences? [13]. With PRA methods, decision-makers can use risk metrics to prioritize risk drivers, rank design alternatives and allocate resources appropriately. NASA has funded many major PRA design methods programs since the mid-1980s. Partial impetus to develop PRA arose from the 1986 Challenger accident report asserting the need to estimate probabilities of failures on Shuttle elements and the 1988 "Post-Challenger Evaluation of Space Shuttle Risk Assessment and Management" recommending immediate application of PRA methods to Shuttle risk management. Early funded programs included the PSAM Project, the PFA Methods Program, probabilistic methods and the QRAS tools [14]. The Saphire tool is also used commonly at NASA and elsewhere for conducting PRA [15]. Some of these tools, such as the finite-element program NESSUS produced by the PSAM project, combine a probability framework with design parameter sensitivity analysis. During the 1990s PRA was applied to designing upgrades to the Space Shuttle [16], conceptual design of second-generation Reusable Launch Vehicles (RLV's) [11] and development of a testbed for manned space missions [12]. These more recent developments attempt to situate PRA methods into early mission design and the spiral design process [2].

Failure Modes and Effects (and Criticality) Analysis (FMEA/FMECA) is a system analysis method to assess risk and reliability issues. The FMEA approach is bottom-up, based on probability of component failure, and requires a more detailed level of system design. Several standard FMEA methodologies exist: from defense and aerospace, the MIL-STD-1629A FMECA standard or the SAE ARP5580 FMEA standard; automotive suppliers use SAE J1739 FMEAs or the Automotive Industry Action Group (AIAG FMEA), Daimler Chrysler, Ford, or GM FMEA methodologies. Other industries generally adopt one of these FMEA standards or others such as IEC 60812 or BS 5760.

The first step in the FMEA process is to break down a system into subsystems and ultimately into individual components, and then to determine the ways in which each component could potentially fail. Each failure mode is evaluated independently, and a determination is made as to what the effect of that failure is at the current level, and then the resulting effect on the entire system. The FMEA analysis is then extended to include information relating to the risk or criticality of these potential system failures, a FMECA. The FMECA is used as part of a risk management process, to assess which failure modes require effort to prevent, mitigate, detect, or ignore. By using FMEAs to assign, categorize and prioritize failure modes, the resulting categories can each have a defined plan of action. For example, high-risk items must be flagged, and a plan to eliminate them can be formulated and deployed. Medium level items may require some type of detection mechanism to be designed. Low risk items perhaps require no action. There are several industry approaches to risk assessment, to quantify the risk levels of failure modes, supported by current commercially available FMEA software, including Mode Criticality, Risk Priority Numbers (RPN), Criticality Rank and Risk Level [17].

Fault Tree Analysis (FTA) is performed using a top down approach. From a high-level failure event, all contributing events that could lead to the occurrence of the top-level event are elaborated. Possible paths from root cause failures to the top-level consequence are captured in a tree structure. Events have an associated probability, usually based on historical data, and are combined using Boolean algebra. The probability of the top-level event can be determined using various mathematical techniques. Fault trees are diagrams showing the chain of events combined using logical gates (and, or, nor, nand, not, xor, voting etc) leading to the top-level failure.

Because FTA is an event-oriented analysis, it can identify more possible failure causes than structure-oriented FMEAs (Failure Modes and Effects Analysis) and RBDs (Reliability Block Diagrams), which are based on component analysis. When performed correctly, FTA often identifies system problems that other design and analytical methods would overlook. Event trees show the chain of events with branches for failure and success paths. Consequences for the system and their likelihood can be determined from the path sequences.

3.4 Tools and Methods for Embedding ISHM into Early Functional Design Stage

One of the critical shortcomings of the methods discussed above is the difficulty in applying them in the early stages of functional design. At the early stage, the system's functional requirements may be firm but selection of specific components to implement functionality has not been made, and hence models of system components and design parameters are not yet available. In order to integrate the health management of these various systems, a modeling paradigm that is capable of representing the desired functionality of the individual systems as well as their interactions is required. One of the most promising approaches to enable analysis of failures and their associated risks is based on a function-based design and failure analysis methodologies, allowing analysis of likely failures even before component selection has begun.

Functional modeling is a form-independent method of representing electro-mechanical systems [8, 9, 18]. A functional model consists of the energy, material and signal flows into and out of a system and the functions that are performed on these flows to transform them from an input to a desired output state. Creating a functional model represented in the Functional Basis language involves five steps, as shown in Figure 6. Through the use of the Functional Basis, functional modeling has been successfully applied to representing such systems and interactions. Function-based modeling relies on verb-noun descriptions of elemental functions based on a standardized taxonomy called the Functional Basis (the Functional Basis is a set of standard function and flow terms developed in a joint effort between the University of Missouri-Rolla, University of Texas-Austin and NIST). A functional model is made by identifying the functions that must be performed to transform the energy, material and information inputs of a system into outputs. This approach enables designers to think through the system layout by following the input and output flows through the main required functions, and generate concepts that eliminate potential failure modes associated with certain functions based on historical data, FMEAs, and expert elicitation [19].

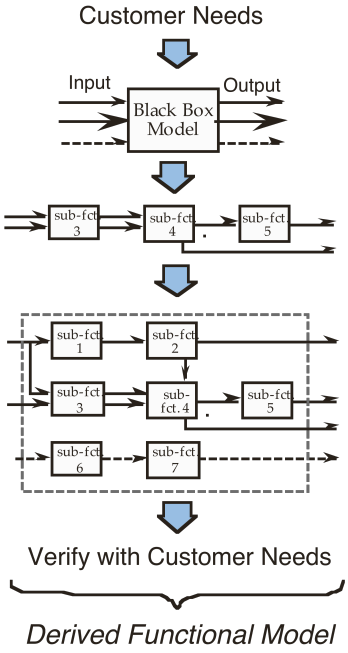

Figure 6. Basic steps of functional modeling.

One example of current research efforts is the identification of failure modes during conceptual design is made possible through the function-failure design method [8]. This method uses a functional model for a system in combination with historic failure information to map the functionality of a system to potential failure modes. A standard taxonomy to describe functionality, namely the Functional Basis [9], is used to

model systems and components at the highest (functional) level, with the intent of providing generic and reusable templates for spacecraft. The method then collects failure data from historical databases and expert elicitation [10, 18], and maps these failures onto function, hence building a knowledge base relating failure modes directly to functionality, bypassing the need to know the details of the design form or solutions.

The function-failure design was also proposed for ISHM co-design, where formal functional modeling techniques are used to enable "co-design" of a system and its health management capability. This method has been proposed to guide the design of ISHM systems, and used in effect to integrate ISHM system functionality design decisions into the design lifecycle. The function-failure analysis was then used to create a function-based failure mode, effect and criticality analysis (FMECA). By applying the function-failure method to the testbed, it was possible to identify potential failure modes for each function during the conceptual design phase. In addition, the function-failure method also identified several areas for improvement in the testbed design. The functional analysis allowed the switching and current flow of the testbed to be outlined very early in the design. As a result, safety concerns such as unsafe operating modes and electrical shock hazards were addressed well before detailed electrical schematics were created. Additionally, the functional analysis served as a platform for identifying the hardware required to meet the testbed requirements. Through collaboration with the hardware designers, the functional analysis was used to reduce the complexity and capacity of the system to a level that met functional requirements while reducing cost and build time [19]. This method is complemented by a risk and uncertainty based design methodology, which takes functional models and the failure modes mapped to each function, and generated a resource allocation vector to minimize risk of functional failures [20]. Such an approach can be used as a precursor to methods such as PRA, to enable its use in early functional design. The method is also extended to model-based reasoning, proposing to derive the diagnostic reasoners for systems starting from functional models, hence taking early design decisions into account [21].

As an example, Figure 7 shows a first attempt to describe the basic functionality of an ISHM system using functional modeling. Currently, a systematic methodology for ISHM co-design is being developed at NASA ARC. The co-design approach will start from a functional model generated from requirements, perform a function-based failure analysis to generate an FMEA type of approach, determine the sensing points and monitoring functions based on the critical functionality and the interfaces between them, perform a system-wide analysis and optimization to determine the impacts of ISHM of the system-level Figures of Merit, reiterate the system and ISHM design based on the insights from this process to hopefully (or perhaps "with a goal of" – in general, one cannot just assume that your procedures will result in a reliable design with a robust ISHM capability, that needs to be proven) result in a reliable system design with a robust ISHM capability.

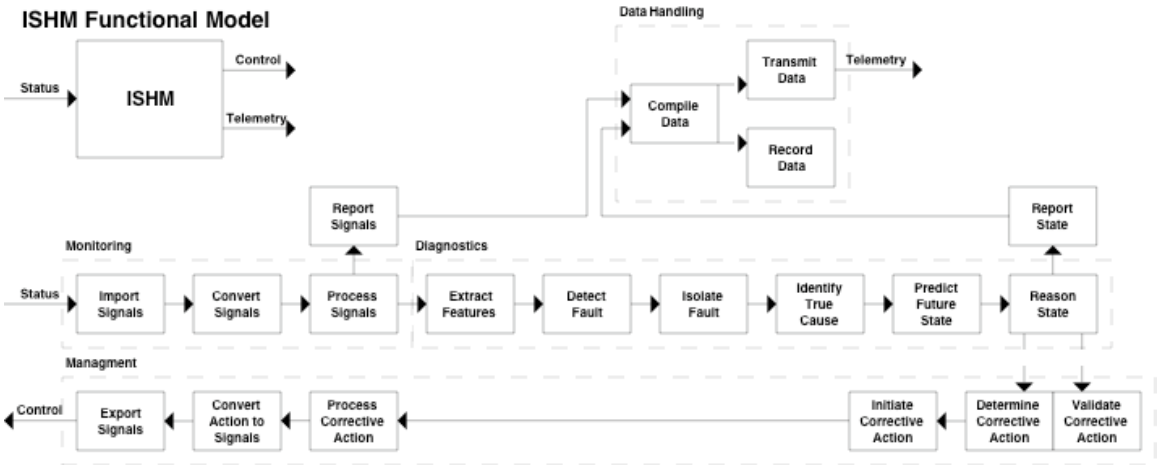

Figure 7. Functional Modeling of the ISHM System.

3.5 Methods for System Analysis and Optimization

ISHM design must anticipate the health management needs of the system throughout its life cycle. Methods must be put in place to deal with residual risks, which remain after the most critical failures have been identified and eliminated from the system design. Such residuals or escapes may not have been mitigated in the failure analysis because of their low probability or low impact, or they may simply be unknowns. Therefore, ISHM design must provide the infrastructure and mechanisms to enable resilience to failures, which occur during operations and for their resolution during maintenance. Where multiple instances of the system exist, such as in a fleet of vehicles, the solution must take this into account. Only then can robustness of the ISHM capability can be achieved.

The process that enables this kind of robustness during the design phase is called the Systems Analysis and Optimization (SA&O) process. SA&O process provides two advantages for ISHM design: (1) The effect of ISHM on the overall safety, maintainability, performance, and cost of the mission can be accurately calculated; (2) During the design phase, engineers can find the 'optimal ISHM architecture' based on quantitative Figures of Merit (FOMs). The latter is particularly important in the early phases of designing a space exploration system where design decisions are still evolving and easy to change. Choosing the optimal ISHM architecture at this stage has the highest impact and offers significant cost reduction downstream as the system design matures. It is critical that this architecture be derived based on reliability, maintainability, and supportability needs and requirements of the ISHM functionality. There are various examples of industry and NASA partnerships that started on this path in the 2nd Generation RLV program; namely, the Honeywell team and the Northrop Grumman team. Although these ideas were not implemented due to the demise of this program, their potential utility has been recognized by industry and NASA ISHM experts. The following subsections describe attempts by industry and NASA to introduce system analysis and optimization into the ISHM design process, and an ongoing effort to enable this goal in the early stages of design.

3.5.1 Design for Testability

Design for Testability is the process used to analyze the degree of observability of a system and modify the design to meet a set of goals for observability. The inherent testability of a system is determined during the design cycle. This analysis is usually performed before any tests are designed and is based on the physical topology of the system and proposed instrumentation locations. Achieved testability is a maintenance characteristic that describes the ability to observe system behavior with the implemented instrumentation.

The electronics industry is a heavy user of DFT methods since optimal built-in-test schemes are of utmost importance in their products. Some of the current DFT tools have roots back to tools developed by the electronics industry in the early 1990s. Industry leaders in this field are TEAMS from Qualtech Systems, Inc. (QSI) [22], and eXpress from DSI [23]. These tools use a model-based approach, which captures the physical connectivity of system components and maps failure modes and instrumentation points onto the dependency graph. Along with testability-figures-of-merit (TFOMS) such as percent detection and percent isolation of modeled faults, other informative characteristics of the system such as ambiguity group sizes and redundant or unused tests are available to system designers. By performing the testability analysis during design, instrumentation placement can be modified to achieve observability goals.

DFT success stories are beginning to be documented in aerospace applications. In 2005, diagnostic software maker QSI was selected by Pratt & Whitney (P&W) to provide real-time on-board diagnostics for F135 jet engines being developed for the F-35 Joint Strike Fighter. In February 2003, QSI also partnered with a Boeing Company-led team to develop the Integrated Engine Diagnostic System (IEDS) for the U.S. Army's Longbow Apache AH-64D helicopter. The QSI toolset provides end-to-end design-to-operations support by utilizing the same multi-signal flowgraph model for testability analysis and for runtime diagnostics. This enables design knowledge capture and ensures the use of consistent system information throughout the system lifecycle.

3.5.2 Honeywell's ISHM Analysis & Optimization Approach

For 2nd Generation RLV, Honeywell was involved in IVHM system analysis and optimization. Honeywell's system analysis and optimization (A&O) process is shown in Figure 2 below [24].

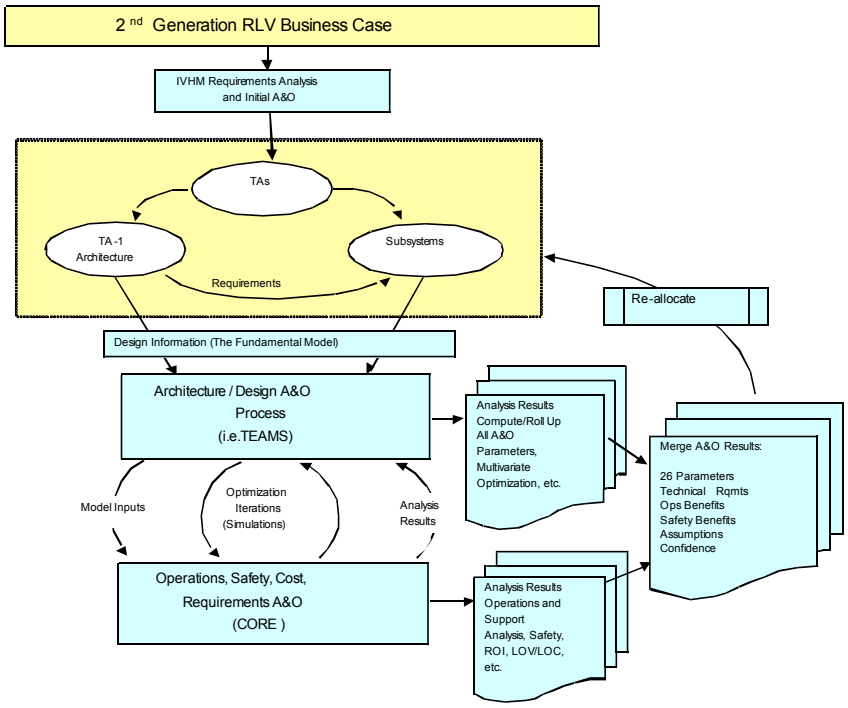

Figure 2: Honeywell's System Analysis and Optimization (A&O) Process.

Honeywell's process revolved around a "fundamental model" (FM), which defined the essential elements that are required to develop, integrate and maintain the health management solution at all levels (e.g., the subsystems, system and system-of- systems levels.) The fundamental model has elements that feed (as inputs) both the systems engineering health management Analysis and Optimization (A&O) activities and the health management solution design activity. The FM captures system design information meeting the requirements from the various Technical Areas (TAs), organizational structures in the Next Generation Launch Technology (NGLT) program including subsystems. The A&O process uses the FM as the initial vehicle design against which to evaluate Features of Merit (FOMs) and Technical Performance Measures (TPMs). Subsystem TPM and FOM metrics are rolled up to the vehicle level. A discrete event simulator such as CORE is used to determine operations, safety and cost metrics for the concept of operations of the fleet of vehicles, from cradle to grave (operations, maintenance and decommissioning). These enterprise-level metrics are fed back to the technical areas for review, revision and reallocation. In this iterative process, A&O evolves in conjunction with the FM, with increasing fidelity and optimization.

The system design or FM information will be specific to an application, however the classes of information of the FM and their uses by A&O need to be clearly determined. At a minimum, the following must be identified: the subsystems and their major components; interactions between subsystems at the system level and between components at the subsystem level; and attributes for components and their interconnections, and how these relate to health management. The FM, which represents system design, is tightly integrated into an A&O solution that utilizes QSI's TEAMS system (see DFT discussion.)

3.5.3 Northrop Grumman's ISHM Analysis & Optimization Approach

The other team for the 2nd Generation Reusable Launch Vehicle (RLV) program was led by Northrop Grumman Corporation (NGC), which developed requirements for optimization of ISHM system performance [25, 26]. The ISHM System Analysis and Optimization (SA&O) work started by a team of people from the NGC and from NASA Ames Research Center (ARC) team has great potential to be applied to the design of ISHM capabilities for Constellation. The aim of this work was to develop a robust methodology that can evaluate different ISHM architectures in an automated fashion to optimize a set of pre-determined Figures Of Merit (FOMs) [27].

The SA&O process developed at NASA ARC and NGC team has been reported to significantly improve the efficiency of the ISHM architecture (For instance, in one case study, the percentage of the total faults that could be detected using the optimized ISHM increased to 75%, up from 12% in the original design). This work has introduced the idea of looking at the FOMs for ISHM and for vehicle design in an integrated fashion. Various models are developed for the case of an X-34 Main Propulsion System that compute the FOMs for ISHM design including: A Design for Testability (DFT) model to determine fault coverage and fault isolation given the sensors; a False Alarm Rate (FAR) model that accounts for possible false alarms introduced by the ISHM system; Maintenance models including Scheduled Maintenance Model that generates an expected turn around time based on predictable maintenance and work schedules, Probability of Unscheduled Maintenance Model that computes a probability that corrective maintenance is required, and Unscheduled Maintenance Duration Model that is made up of 'fault detection time' and 'Fault correction time'; a Discrete Event Simulation Model that performs a discrete event simulation to predict the time required to prepare the RLV for the next mission; a Probabilistic Risk Assessment Model that computes the Loss of Mission (LOM) using a fault tree of vehicle subsystems that includes ISHM [27, 28].

Important safety and reliability metrics are Probability of Loss of Crew (PLOC), Probability of Loss of Vehicle (PLOV), Probability of Loss of Payload (PLOP) and Probability of Loss of Mission (PLOM). Reliability also determines availability (including turn-around time) and maximum mission rate. Cost metrics include costs due to system design, infrastructure, system acquisition and disposal and recurring operations costs. These safety, reliability and cost metrics are the FOMs in the objective function, to be minimized in deriving an optimal solution. Some minimum safety level will be required, invalidating any solution which does not meet this need. Safety margin provides the basis for optimization.

Discrete Event Simulation (DES) tools, such as Arena and CORE, provide operations models which may be used to automate SA&O. The DES models every item that needs to be maintained as well as probability of unscheduled maintenance, labor hours and generates time taken to execute maintenance events. For example, a DES may use a Gaussian probability distribution to generate variability on inputs to turn-around time. A DES of loss of mission (LOM) may combine a PRA event tree (which indicates probability of faults) with the DFT application (which given a sensor set and algorithm is the probability of detecting it).

3.5.4 Multi-Objective and Multi-Disciplinary Optimization Framework

Although the SA&O approach has great value for designing ISHM functionality into Exploration Mission systems, the use of the methods and tools is very time-intensive and requires considerable knowledge and expertise. To bring practical value, a quick trade study environment must be available to enable system analysis and optimization.

The effective automation of such a process inevitably requires a proper optimization scheme. For systems analysis and optimization, a multilevel optimization strategy was proposed by the NGC team, shown in Figure 3 below [24, 29].

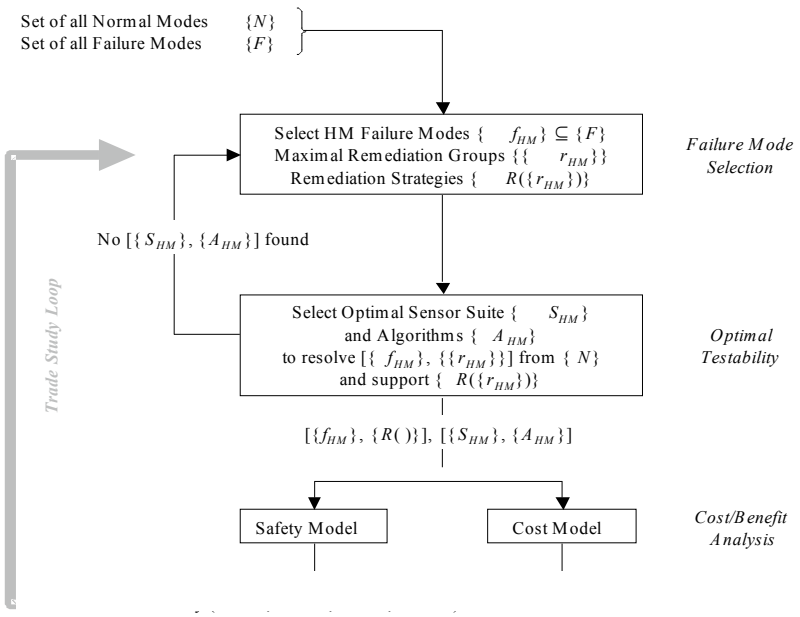

Figure 3. NGC Multi-Level Optimization Strategy.

In this strategy, the failure modes that must be detectable during operations are identified, as well as their maximal fault isolation groups. This step is conducted by reliability and maintainability systems engineers, based on FMECA, maintainability analyses, and IVHM Value Analysis (IVA). In the next step, a sensor placement configuration together with processing algorithms that are capable of detecting the identified failures are selected. The candidate solution (failures+sensors+algorithms) is then evaluated against an objective function. Alternate solutions can then be traded-off to select the optimal solution. The objective function captures what it means for a system to be successful. NGC's optimization algorithm has the advantage that it can potentially be formalized and automated. However, the optimization needed for the SA&O problem domain needs to address two additional aspects:

- Design of an ISHM is multidisciplinary by nature: Designing an ISHM that encompasses all subsystems of a space mission is the result of interaction among engineers and managers from different disciplines with their own domain expertise. The general process of analyzing an ISHM system involves complex numerical simulations, each addressing a different aspect of the overall system. These distinct disciplines often share certain design parameters, but also contain local parameters that are not necessarily relayed to other disciplines or the system-level managers. Therefore, the SA&O process needs to be structured in a two-level hierarchical architecture with shared (global) as well as local design parameters that mimics the autonomy of subsystem engineering groups as well as their interactions with each other and with the system-level design requirements (for a review of multidisciplinary design techniques in the aerospace industry, see [30].)
- Design of an optimal ISHM is multiobjective by requirement: NASA considers multiple Figures Of Merit (FOM's) in both subsystem and system levels. These design objectives are conflicting and incommensurable (they address different aspects of performance in a space mission). Because of the tradeoff among these various objectives, the SA&O process must address a multi-objective optimization strategy that aims to capture the entire Pareto frontier (or as much of the Pareto frontier as possible) in an attempt to generate a set of design alternatives to represent the tradeoff among various objectives(for a thorough review of multiobjective optimization techniques, see [31]). The previous SA&O efforts were only capable of generating a 'point-design' and were not able to find a suite of design alternatives [27].

To address these two aspects, a multi-disciplinary and multi-objective system analysis and optimization (MMSA&O) framework is currently being developed in the Discovery and Systems Health area at NASA ARC. This framework is intended to guide the integrated process and enable the trade analysis for ISHM design. The main objectives are categorized as: 1-Performance, 2-Costs, and 3- Risks. At the lower-level, distinct disciplines (sub-problems) are considered: 1- ISHM itself; 2- RLV system; and 3- Everything else is lumped into one sub-problem. The proposed MMSA&O approach need not be specific to a specific architecture and should be easily generalized to solve similar problems with different discipline breakdowns or with more than two levels of decomposition. The solutions from sub-problems are rolled up to the top-level for integration. However, since each sub-problem is solved independently in every iteration, the design solutions from various sub-problems are biased in distinct directions in the design space. The sub-problems are individual multi-objective optimization problems that can be solved using any appropriate optimization technique. Figure 4 shows the overall schematic of a proposed MMSA&O process currently being developed at NASA ARC [28].

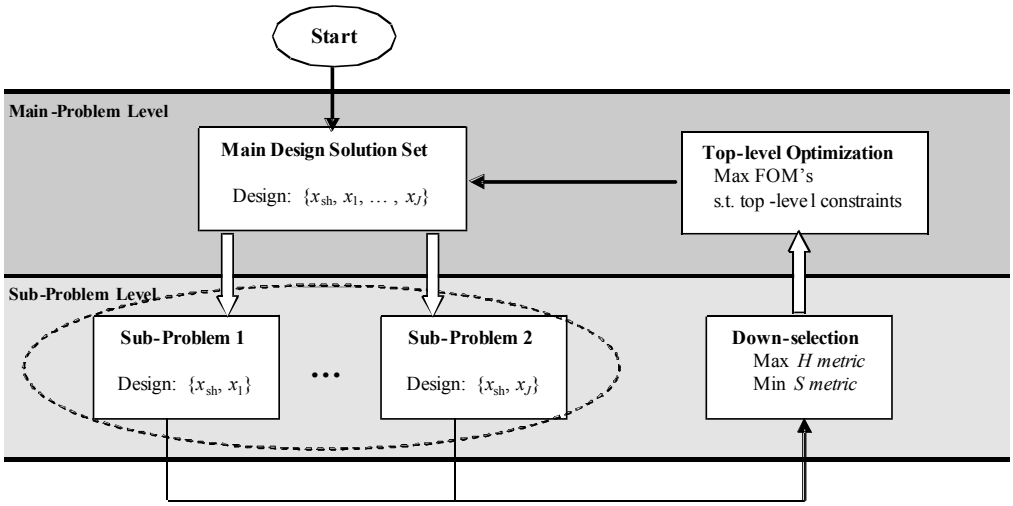

Figure 4. Overall schematic of MMSA&O.

In order to demonstrate the MMSA&O process, the example of an X-34 Main Propulsion Subsystem (MPS) was used. The MPS was designed to be part of the boosters for a Re-usable Launch Vehicle (A Reusable Launch Vehicle is the first stage of a Two-Stage-To-Orbit (TSTO) vehicle which also has the ability to dock to the International Space Station and returns to Earth) [32]. The models used were originally developed by Datta et al. [27] as part of the initial study of the SA&O process. Figure 5 shows a hierarchical decomposition of the generalized X-34 launch system. The details of this approach are presented in [28].

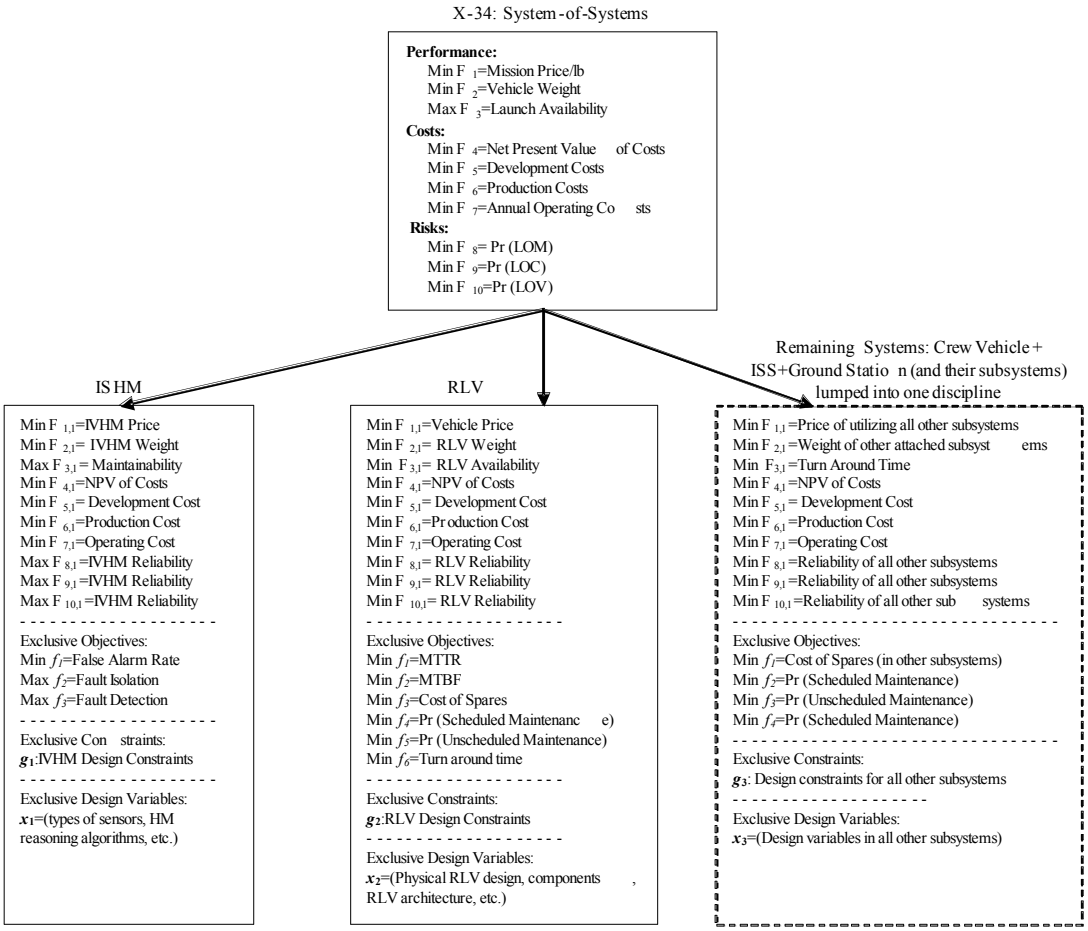

Figure 5. X-34 System-of-Systems is decomposed to: 1) ISHM; 2) vehicle; 3) everything else.

4 SUMMARY AND RECOMMENDATIONS

For NASA's ambitious Exploration Mission where ISHM will be a critical capability, designing the ISHM functionality into the overall systems and vehicles, from the very beginning of the system-level design stage, and including ISHM as one of the main functions of the overall system are required to design and implement robust ISHM systems. This paper provided an overview of possible design practices and methods that might be considered as a means to ensure robust ISHM design and implementation. The overview provided in this paper can be summarized in terms of two main recommendations for NASA's Exploration Mission Program:

1. The Design Approach:

Standard systems engineering practices must be implemented for ISHM co-design with all other subsystems. In addition, new methods must be developed and implemented to enable an integrated systems-level engineering and design framework for ISHM design simultaneous with the vehicle and systems to meet performance, reliability and cost requirements. Methods should be developed and implemented so that co-design can commence at the functional design stage, and rapid trade studies can be performed to assess impact of ISHM on system level FOMs.

There are two aspects to this recommendation: 1) To enable ISHM and Constellation Systems integration in the early phases of design, systematic function-based methods must be implemented. Function-based approaches start with the operational concept, and describe the main functionality independent of the solutions, before design decisions are finalized. Traditional failure analysis and risk assessment methods can be done early by starting with functional models of ISHM and Exploration systems. Such methods are employed in many other industries and have been proven to provide a systematic way of thinking and describing the design at the earliest stages. 2) To enable an integrated analysis and optimization of the ISHM and Exploration systems, the effect of ISHM on the overall safety, maintainability, performance, and cost of the mission must be accurately calculated. There are various examples of industry and NASA partnerships that started on this path in the 2nd Generation RLV program; namely, the Honeywell team and the Northrop Grumman team. These ideas are promising but have not yet been implemented and need to be validated on real projects.

2. Lifecycle Considerations:

All stakeholders should be involved in the requirements development, operation concepts, design process to assess the FOMs and to ensure robust design and operation of ISHM systems. To integrate with other phases of the mission lifecycle, as a minimum, the following communities need to be involved: Ops (flight and ground), engineering, R&D, flight crews, requirements team, S&MA, operational personnel, maintenance personnel.

If NASA's Exploration mission is to be realized within available resources, it cannot afford to follow the example of previous major programs where operations and maintenance costs and risks became much larger than initially projected during Phase A initial design. Decisions in various phases such as design, operations and maintenance have a significant impact on the reliability, affordability, and performance of the overall ISHM system. Decisions should be made with all the data and experts available instead of after the design and testing process is completed, which will result in significant savings in cost and reduction in risk. In addition to supporting the design of reliable systems, with ability to respond to failures during operations and hooks for system maintenance, the initial design must be examined in the context of the full system lifecycle.

5 ACKNOWLEDGMENT

The author would like to thank Sandra Hayden for providing the background and insights about the ISHM work with Northrop and Honeywell for the 2nd Gen RLV Program, Dr. Ann Patterson-Hine for her insights about Design for Testability, Dr. Eric Barszcz and Dr. Ali Farhang Mehr for their input and Dr. Serdar Uckun for his comments on the paper.

6 REFERENCES

1. DARPA. *JSF: A DARPA Perspective*. in *Intelligent Systems Health Management Technical Interchange Meeting, Sensors for Industry Conference*. 2005. Houston, TX.
2. Tumer, I.Y., F. Barrientos, and A.F. Mehr. *Towards risk based design (RBD) of space exploration missions: a review of RBD practice and research trends at NASA*. in *International Design Engineering Technical Conferences*. 2005. Long Beach, CA.
3. Feather, M.S. and S.L. Cornford, *Quantitative risk based requirements reasoning.* Requirements engineering journal, 2003. **8**(4): p. 248-265.
4. Sobieski, J.S. and R.T. Haftka, *Multidisciplinary aerospace design optimization: a survey.* Structural optimization, 1997. **14**: p. 1-23.
5. Sobieski, J.S., et al. *Advancement of bi-level integrated system synthesis (BLISS)*. in *38th AIAA Aerospace Sciences Meeting and Exhibit*. 2000.

6. Pu, P. and D. Lalanne. *Design visual thinking tools for mixed initiative systems.* in *Intelligent user interfaces*. 2002. San Francisco, Ca.
7. Reddy, R. and F. Mistree. *Modeling uncertainty in selection using exact interval arithmetic*. in *Design theory and methodology*. 1992.
8. Tumer, I.Y. and R.B. Stone, *Mapping Function to Failure During High-Risk Component Development.* Research in Engineering Design, 2003. **14**: p. 25-33.
9. Stone, R.B., I.Y. Tumer, and M. VanWie, *The function-failure design method.* Journal of Mechanical Design, 2005. **127**(3): p. 397-407.
10. Uder, S., R.B. Stone, and I.Y. Tumer. *Failure Analysis in Subsystem Design for Space Missions*. in *International Design Engineering Technical Conferences, Design Theory and Methodology Conference*. 2004.
11. Go, S. and D. Mathias. *A top-down risk assessment tool for a reusable launch vehicle development program*. in *41st AIAA Aerospace Sciences Meeting & Exhibit*. 2003. Reno, NV.
12. Jones, H.W. and R.L. Dillon-Merill. *Reducing the Risk of Human Space Missions with INTEGRITY*. in *33nd International Conference on Environmental Systems*. 2003. Vancouver, British Columbia, Canada.
13. Stamatelatos, M. and G. Apostolakis, *Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners v1.1*. 2002, NASA, Office of Safety and Mission Assurance.
14. Townsend, J.S. and C. Smart. *Reliability/risk analysis methods and design tools for application in space programs*. in *AIAA Defense and Civil Space Programs Conference and Exhibit*. 1998. Huntsville, AL.
15. SAPHIRE, *Systems Analysis Programs for Hands-on Integrated Reliability Evaluation,* http://saphire.inel.gov.
16. Greenfield, M.A. *NASA's Use of Quantitative Risk Assessment for Safety Upgrades*. in *IAA Symposium*. 2000. Rio de Janeiro, Brazil.
17. Palady, P., *FMEA - Failure Modes & Effect Analysis - Predicting & Preventing Problems Before They Occur*, R.S. Corporation, Editor. 2005.
18. Stock, M.E., R.B. Stone, and I.Y. Tumer, *Linking product function to historical failures to improve failure analysis in design.* Research in Engineering Design, 2005. **In Print.**
19. Hutcheson, R. and I.Y. Tumer. *Function-based design of a spacecraft power system diagnostics testbed*. in *ASME International Mechanical Engineering Congress and Exposition (IMECE)*. 2005. Orlando, FL.
20. Mehr, A.F. and I.Y. Tumer. *A new approach to probabilistic risk analysis in concurrent and distributed design of aerospace systems*. in *Internation Design Engineering Technical Conferences, Design Automation Conference*. 2005. Long Beach, CA.
21. Hutcheson, R.S. and I.Y. Tumer. *Function-Based Co-Design paradigm for Robust Health Management*. in *International Workshop on Structural Health Monitoring (IWSHM)*. 2005. Stanford, CA.
22. QSI, Q.S.I., *Testability Engineering and Maintenance System (TEAMS) Tool.* http://www.teamqsi.com/prods.html.
23. International, D., *eXpress Tool.* http://www.dsiintl.com.
24. Dixon, R.W. *Demonstration of an SLI Vehicle Health Management System With In-flight and Ground-based Subsystem Interfaces*. in *IEEE Aerospace Conference*. 2003. Big Sky, Montana.
25. NGC, *TA-5 Risk Reduction Integrated Vehicle Health Management IVHM Systems Analysis and Optimization Process Steps (Milestones 2 & 3)*. 2002.
26. Brown, S., *Baseline requirements for optimization of ISHM system performance*. 2001, Northrop Grunman.
27. Datta, K., et al. *An IVHM Systems Analysis and Optimization Process*. in *IEEE Aerospace Conference*. 2003. Big Sky, Montana.
28. Mehr, A.F., I.Y. Tumer, and E. Barszcz. *Optimal design of ISHM for improving the safety of NASAs exploration missions: a multidisciplinary approach*. in *World Congress on Structural and Multidisciplinary Optimization*. 2005. Rio De Janeiro, Brazil.
29. Christenson, R.L., M.A. Nelson, and J.P. Butas. *Rocket Engine Health Management – Early definition of critical flight measurements*. in *39th AIAA/ASME/SAE/ASEE Joint Propulsion Conference and Exhibit*. 2003.

30. Sobieszczanski-Sobieski, J. and R.T. Haftka, *Multidisciplinary aerospace design optimization: A survey of recent developments*. Structural Optimization, 1997. **14**(1): p. 1-23.
31. Fonseca, C.M. and P.J. Fleming. *On the performance assessment and comparison of stochastic multiobjective optimizers*. in *Fourth international confernece on parallel problem solving from nature*. 1996. Berlin, Germany.
32. R. H. Champion, J. and R.J. Darrow. *X-34 main propulsion system design and operation*. in *AIAA*. 1998.